

Arizona Corporation Commission
DOCKETED

MAR 20 2012



ORIGINAL



0000135289

Elizabeth A. Kelley, MA
Director, Electromagnetic Safety Alliance, Inc.

3031 N. Gaia Place
Tucson, Arizona, U.S.A. 85745
kelley_45@msn.com / 520 743-0125

RECEIVED

2012 MAR 20 A 11: 16

March 15, 2012
AZCC COMMISSION
DOCKET CONTROL

To: AZCC Docket Control Center
1200 West Washington St
Phoenix, Arizona 85007

Ref: Public Comments submitted on AZCC metering privacy proposal - Docket No. E-00000C-11-0328

These comments represent my opinion as Director of the Electromagnetic Safety Alliance, Inc. These comments do not necessarily represent the views of Arizonans for Safer Utility Infrastructure, for which I serve as Co-coordinator.

I appreciate the efforts put forth by the AZCC Utilities Division in developing this privacy proposal. The current version seems very preliminary and lacks detail. I look forward to reviewing a more detailed proposal at a later date.

Proposal: Wireless meters are more susceptible to data hacking and cyber security breaches. There are no policies in place to assure the right to privacy under the 4th Amendment of the U.S. Constitution for residential and small commercial property owners and tenants. Therefore, it is highly recommended that the Arizona Corporation Commission impose a one year moratorium on smart metering development and operations in order that it can evaluate alternatives to wireless meters, such as fiber optics or wired phone lines, and other technological solutions in support of the energy efficiency and conservation plan goals and assure that proper privacy policies are in place. Meanwhile, property owners should be permitted to opt out or have their analog meters reinstalled, upon request.

Note: The AZCC did not mandate that the electrical utilities in Arizona install wireless smart meters in its 2010 energy efficiency and conservation plan.

General comments:

1. Staff asks, "Does the draft proposed guidelines adequately address privacy concerns? I do not think it is possible to know at this point. Federal government guidance is incomplete. Here are some weaknesses in the current proposal:
 - These privacy policy proposals seem to emphasize the needs and the rights of the utilities over the needs and rights of residential and small commercial customers.
 - Currently there are no national privacy rules for residential and small commercial buildings where the smart meters are being installed. This may mean that the states and the utilities are free to set their own rules. Or, this may mean that national standards are

forthcoming. Due to the wireless mode of data transmissions and the preferential use of third party contractors to handle utility usage data, these data are potentially vulnerable to hacking and unauthorized sharing of personal and household data. This is why military installations, universities and certain research and manufacturing plants are creating their own mini-grids with a secure portal to the internet. Residential and small commercial property owners and their tenants deserve the same privacy and security protections as these groups have.

- By comparison the federal HIPAA rules that set uniform standards to protect patient health information privacy are comprehensive and require patient disclosure and advance permission, documentation, and sanctions for noncompliance. I think these proposed privacy guidelines for metering ought to be tightened considerably in order to protect the privacy of residential and small commercial building occupants, whether property owners or tenants.

- A February 2012 Congressional Research Service report, entitled "Smart Meter Data: Privacy and Cyber security"¹, outlines the privacy and security issues of the data collected by the new AMI technology infrastructure (AMI, Advance Metering Infrastructure) which is the latest technological metering option available and is being deployed nationwide. The authors recognize that "detailed electricity usage data offers a window into the lives of people inside of a home by revealing what individual appliances they are using and the transmission of the data potentially subjects this information to interception or theft by unauthorized third parties or hackers. The authors warn, as the technology evolves, privacy and cyber security issues are likely to evolve and that "unforeseen consequences under federal law may result from the installation of smart meters and the communications technologies that accompany them." The 4th Amendment of the U.S Constitution is specifically mentioned throughout and many federal legal citations are referenced in this report. In sum, I think there are many unanswered questions and concerns that should first be addressed before installing smart meters that communicate with the smart grid infrastructure.

2. In the absence of mandatory rules how can the AZCC assure that all utilities in the state, whether corporately, municipally, cooperatively, or tribally owned, will comply with them? I understand that only the investor owned utilities are required to meet AZCC rules but since these corporate owned utilities are also part of national corporations, corporate headquarter rules may not be consistent with the AZCC rules or may preempt state guidelines.
3. What does the use of term "guidelines" signify in relationship to this proposal? Does this mean the guidelines are voluntary or mandatory for compliance by individual utilities? If these guidelines are mandatory, how will the state ensure regulatory compliance and what sanctions are in place to address noncompliance with these guidelines? If these guidelines are voluntary, how would the AZCC address issues raised related to them if they cannot be enforced?
4. Even if these guidelines were mandatory and enforceable for all electrical utilities, whether they are public and private, that do business in Arizona, it would be disingenuous to assume that they were capable of protecting privacy. The cognizant federal agencies (DOE, Commerce/NIST and FCC) who along with the North American Electrical Reliability Council, who are taking the lead over the smart grid infrastructure deployment nationally, are in the early research and development mode now in year 2 of federal smart grid grant-making, and do not have cyber-

security or national interoperability standards in place yet. This technology is still considered experimental and security and privacy protections are not in place yet. Some cities and counties have declared moratoriums on further smart meter installations because of this. Even though these moratoriums are nonbinding, they symbolize the deep dissatisfaction many local governments and elected officials have with the way the smart grid is being deployed. State ACLU Chapters (Vermont and Hawaii), the Electronic Frontier Foundation, TURN (The Utility Reform Network) in California, and other groups are challenging smart meter deployment on constitutional and other federal and state legal grounds.

Since the September 2011 workshop, when I submitted a petition signed by over 90 Arizonans and over 30 Arizonans testified before the AZCC Commissions regarding their concerns about privacy, health and pocketbook issues, the electrical utility companies in Arizona have continued to install smart meters, even against previously expressed wishes of property owners. I receive several inquiries a week from people and have heard many horrifying stories about how this has affected people adversely. It is clear to me that people feel unheard and at times, abused. This issue needs to be resolved promptly and fairly. For those whose health and well being are being adversely affected by the deployment of wireless meters, this is an urgent matter as involuntary exposure to smart meters can cause functional impairments, such as an inability to sleep at night or, the people's right to private enjoyment of one's property taken away from them.

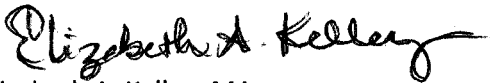
Opposition to the deployment of smart meters in Arizona as well as in other states across the country is growing, is having a chilling effect on the people and is adding to the crisis of confidence people have towards their elected representatives and the role of government in their lives. I hope that the individual utilities and the AZCC will take my opinions expressed here seriously into account in the coming weeks.

In sum, I think the adoption of a privacy policy is premature given the complexity of the issue and the fact that the technology is evolving rapidly that may result in more secure data handling. By taking more time, an adequate policy may be possible.

In addition to this original signed statement, 13 copies of this original submission, the cover page and abstract of the CRS report, and, one complete copy of the CRS report are attached

Please add my name to the service list for this Docket No. No. E-00000C-11-0328.

Sincerely,


Elizabeth A. Kelley, MA

#####

ⁱ Congressional Research Service, "Smart Meter Data: Privacy and Cyber security" 7-5700, R42338, February 3, 2012.
www.crs.gov.



Smart Meter Data: Privacy and Cybersecurity

Brandon J. Murrill
Legislative Attorney

Edward C. Liu
Legislative Attorney

Richard M. Thompson II
Legislative Attorney

February 3, 2012

Congressional Research Service

7-5700

www.crs.gov

R42338

CRS Report for Congress
Prepared for Members and Committees of Congress

Summary

Fueled by stimulus funding in the American Recovery and Reinvestment Act of 2009 (ARRA), electric utilities have accelerated their deployment of smart meters to millions of homes across the United States with help from the Department of Energy's Smart Grid Investment Grant program. As the meters multiply, so do issues concerning the privacy and security of the data collected by the new technology. This Advanced Metering Infrastructure (AMI) promises to increase energy efficiency, bolster electric power grid reliability, and facilitate demand response, among other benefits. However, to fulfill these ends, smart meters must record near-real time data on consumer electricity usage and transmit the data to utilities over great distances via communications networks that serve the smart grid. Detailed electricity usage data offers a window into the lives of people inside of a home by revealing what individual appliances they are using, and the transmission of the data potentially subjects this information to interception or theft by unauthorized third parties or hackers.

Unforeseen consequences under federal law may result from the installation of smart meters and the communications technologies that accompany them. This report examines federal privacy and cybersecurity laws that may apply to consumer data collected by residential smart meters. It begins with an examination of the constitutional provisions in the Fourth Amendment that may apply to the data. As we progress into the 21st century, access to personal data, including information generated from smart meters, is a new frontier for police investigations. The Fourth Amendment generally requires police to have probable cause to search an area in which a person has a reasonable expectation of privacy. However, courts have used the third-party doctrine to deny protection to information a customer gives to a business as part of their commercial relationship. This rule is used by police to access bank records, telephone records, and traditional utility records. Nevertheless, there are several core differences between smart meters and the general third-party cases that may cause concerns about its application. These include concerns expressed by the courts and Congress about the ability of technology to potentially erode individuals' privacy.

If smart meter data and transmissions fall outside of the protection of the Fourth Amendment, they may still be protected from unauthorized disclosure or access under the Stored Communications Act (SCA), the Computer Fraud and Abuse Act (CFAA), and the Electronic Communications Privacy Act (ECPA). These statutes, however, would appear to permit law enforcement to access smart meter data for investigative purposes under procedures provided in the SCA, ECPA, and the Foreign Intelligence Surveillance Act (FISA), subject to certain conditions. Additionally, an electric utility's privacy and security practices with regard to consumer data may be subject to Section 5 of the Federal Trade Commission Act (FTC Act). The Federal Trade Commission (FTC) has recently focused its consumer protection enforcement on entities that violate their privacy policies or fail to protect data from unauthorized access. This authority could apply to electric utilities in possession of smart meter data, provided that the FTC has statutory jurisdiction over them. General federal privacy safeguards provided under the Federal Privacy Act of 1974 (FPA) protect smart meter data maintained by federal agencies, including data held by federally owned electric utilities.

A companion report from CRS focusing on policy issues associated with smart grid cybersecurity, CRS Report R41886, *The Smart Grid and Cybersecurity—Regulatory Policy and Issues*, by Richard J. Campbell, is also available.